From: Ritchey, Gail (COT)
Sent: Wednesday, December 26, 2007 2:26 PM
To: COT Constitutional CIO Security Contacts; COT Cabinet CIO Security Contacts; CTC Members
Cc: COT Exchange Administrators; COT Security Alert Contacts; COT Security Contact COT-Support; COT Security Contact Pass; COT Security Contact Self-Support; COT Technical Contacts; SecurityContacts Group
Subject: COT Security Alert: Storm Botnet Danger

COT Security Alert

The COT Security Administration Branch is alerting all Commonwealth email and Internet users to the following threat reported by the SANS (SysAdmin, Audit, Network, Security) Institute . A new ploy is being used to spread the Storm Botnet. This current version uses a New Year's-themed e-card which directs the user to "uhavepostcard.com". This URL should not be visited as it will infect the user's computer with malware ("happy2008.exe"). The message comes with one line of text used for both the subject and message text. The messages used include the following:

- Happy 2008!
- Happy New Year!
- New Hope and New Beginnings
- New Year Ecard
- Opportunities for the new year
- Happy New Year to <email address>

Several other one-line message-texts known to be used may be found at www.sans.org/diary. This list will probably grow and the domain IP address will likely change often as the offenders attempt to avoid defensive web and email blocks.

Users are advised not to open spam on any occasion, and never to click on attachments in emails unless the source is verified. To do so can result in an infection which could potentially spread across the state government network.

NOTICE: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

Commonwealth Office of Technology
Division of Technical Services
Security Administration Branch
120 Glenn's Creek Rd., Frankfort, KY 40601
COTSecurityServices@ky.gov
http://ky.gov/got/security/